RSAC 2025 Conference

Many Voices.
One Community.

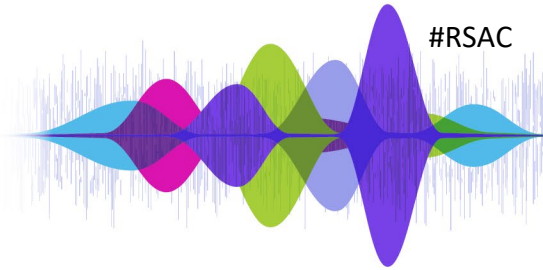
SESSION ID: USENIX-M06A

Logic Gone Astray: A Security Analysis Framework for the Control Plane Protocols of 5G Basebands

Kai Tu

SyNSec Research Lab
The Pennsylvania State University

Disclaimer

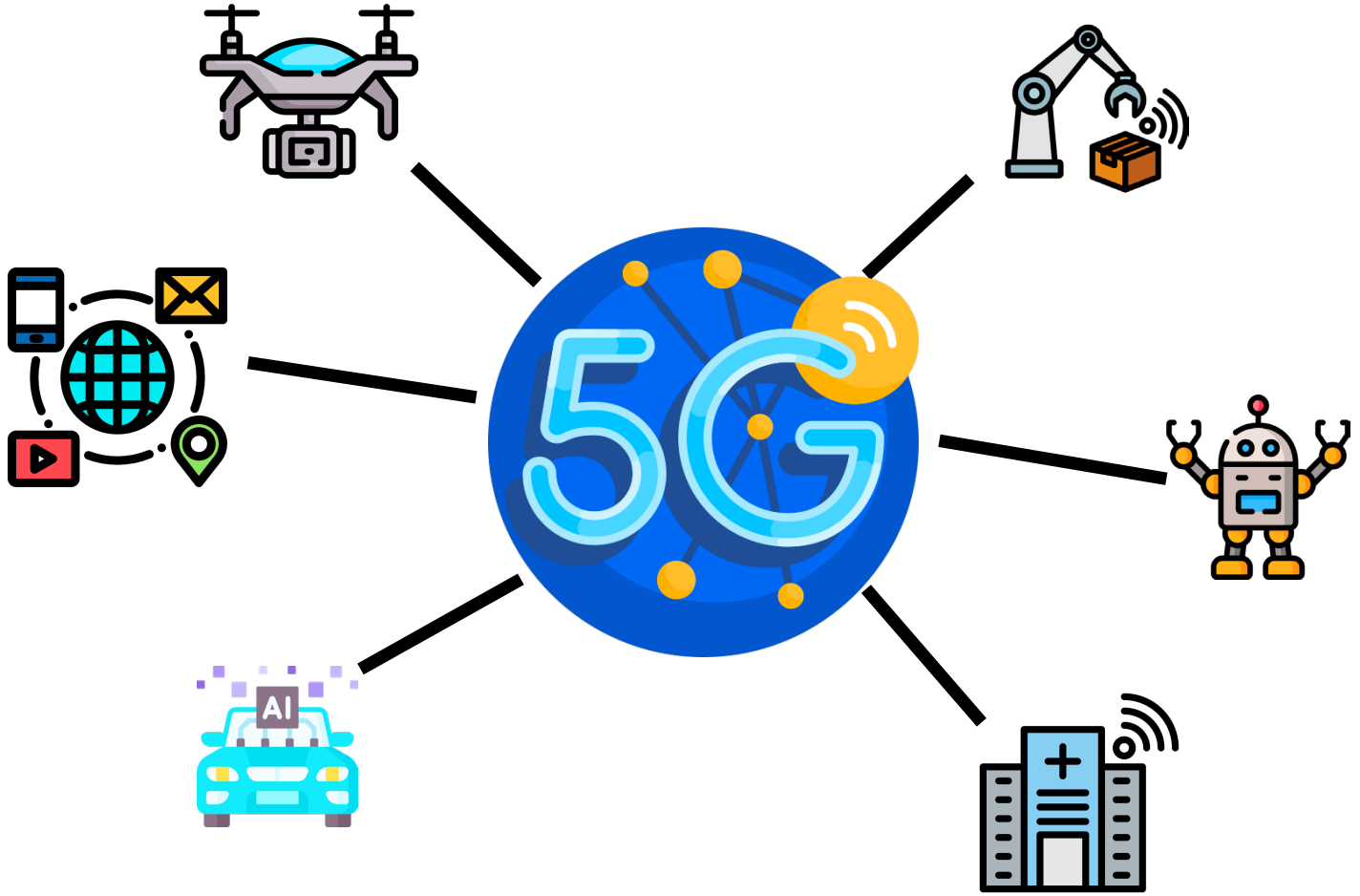


Presentations are intended for educational purposes only and do not replace independent professional judgment. Statements of fact and opinions expressed are those of the presenters individually and, unless expressly stated to the contrary, are not the opinion or position of RSA Conference LLC or any other co-sponsors. RSA Conference LLC does not endorse or approve, and assumes no responsibility for, the content, accuracy or completeness of the information presented.

Attendees should note that sessions may be audio- or video-recorded and may be published in various media, including print, audio and video formats without further notice. The presentation template and any media capture are subject to copyright protection.

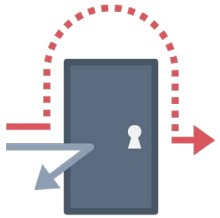
© 2025 RSA Conference LLC or its affiliates. The RSAC and RSAC CONFERENCE logos and other trademarks are proprietary. All rights reserved.

5G Cellular Networks



Why is 5G Baseband Security Important?

- Users will run into critical problems if basebands are not secure.



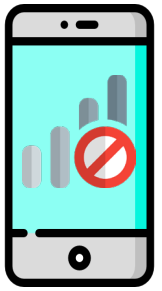
'5Ghoul' Vulnerabilities Haunt Qualcomm, MediaTek 5G Modems

Source: https://www.securityweek.com/5ghoul-vulnerabilities-haunt-qualcomm-mediatek-5g-modems/

Your Phone's 5G Connection Is Vulnerable to Bypass, DoS Attacks

Wireless service providers prioritize uptime and lag time, occasionally at the cost of security, allowing attackers to take advantage, steal data, and worse.

Source:https://www.darkreading.com/mobile-security/your-phone-s-5g-connection-is-exposed-to-bypass-dos-attacks



- Compromised 5G device may also affect other components in 5G.

Exploits & Vulnerabilities

Attacks on 5G Infrastructure From Users' Devices

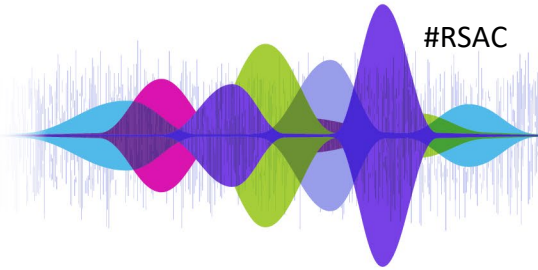
Source: https://www.trendmicro.com/en_us/research/23/i/attacks-on-5g-infrastructure-from-users-devices

We are curious…

How secure are the 5G devices?

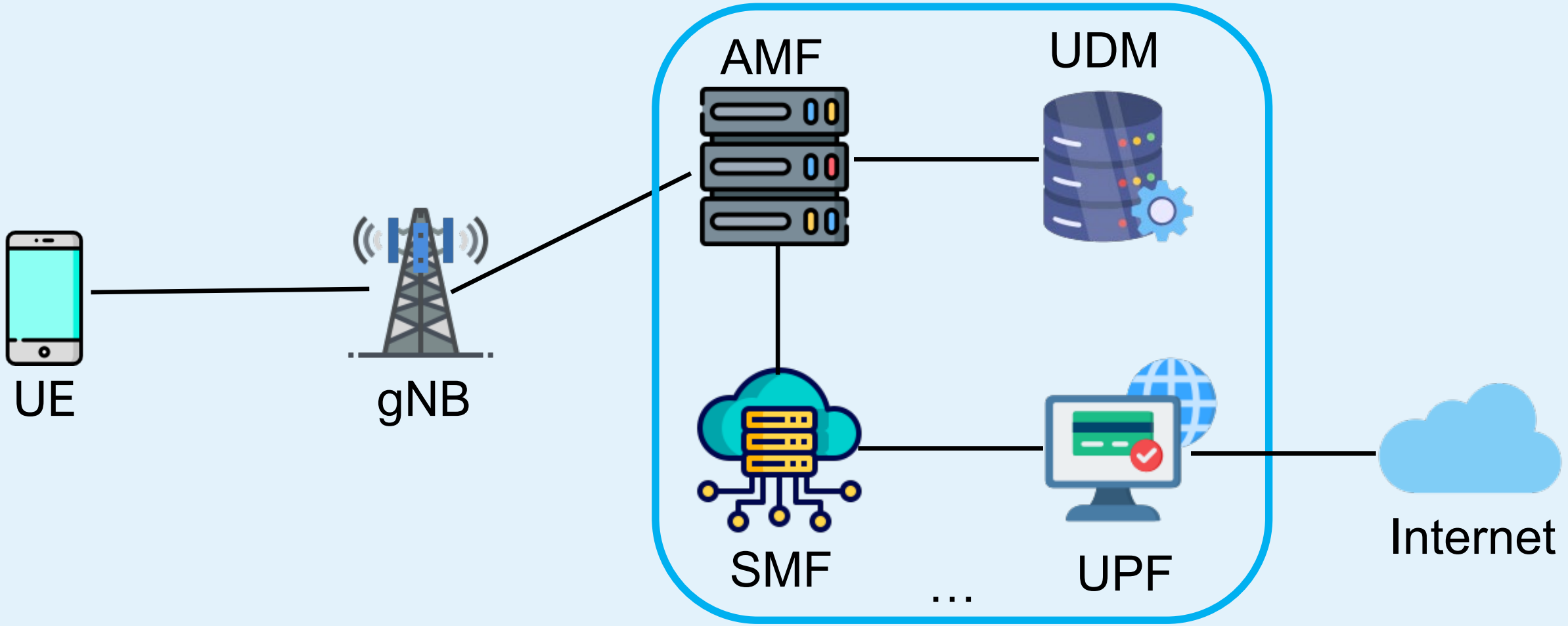
Can we develop an automated way to test them?

What We Are Going to Talk About Today

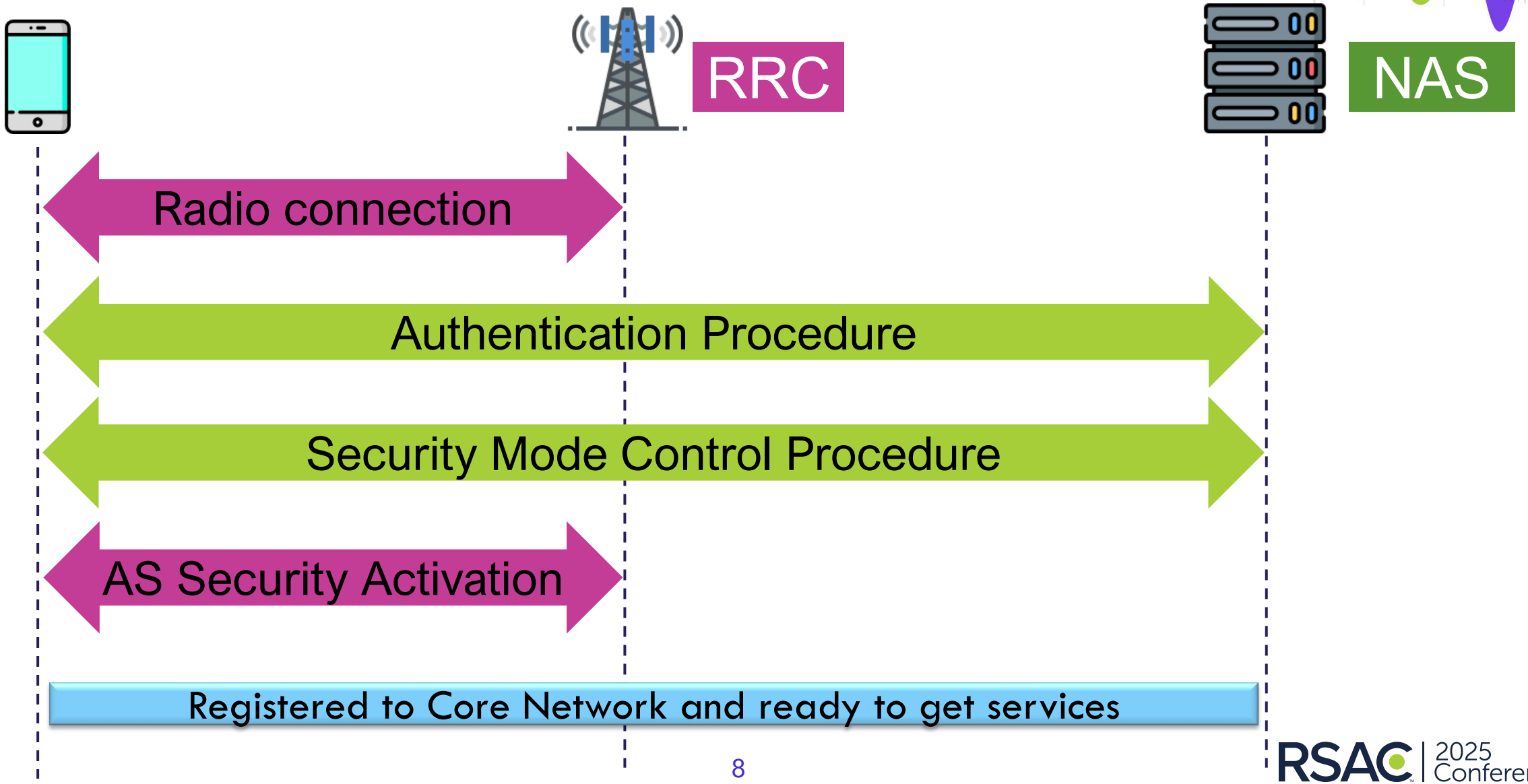


- 5G cellular network overview
- Workflow of our automated 5G baseband testing tool
- Summary of findings
- 5G AKA bypass end-to-end exploitations demos
- Impact and status
- Takeaways

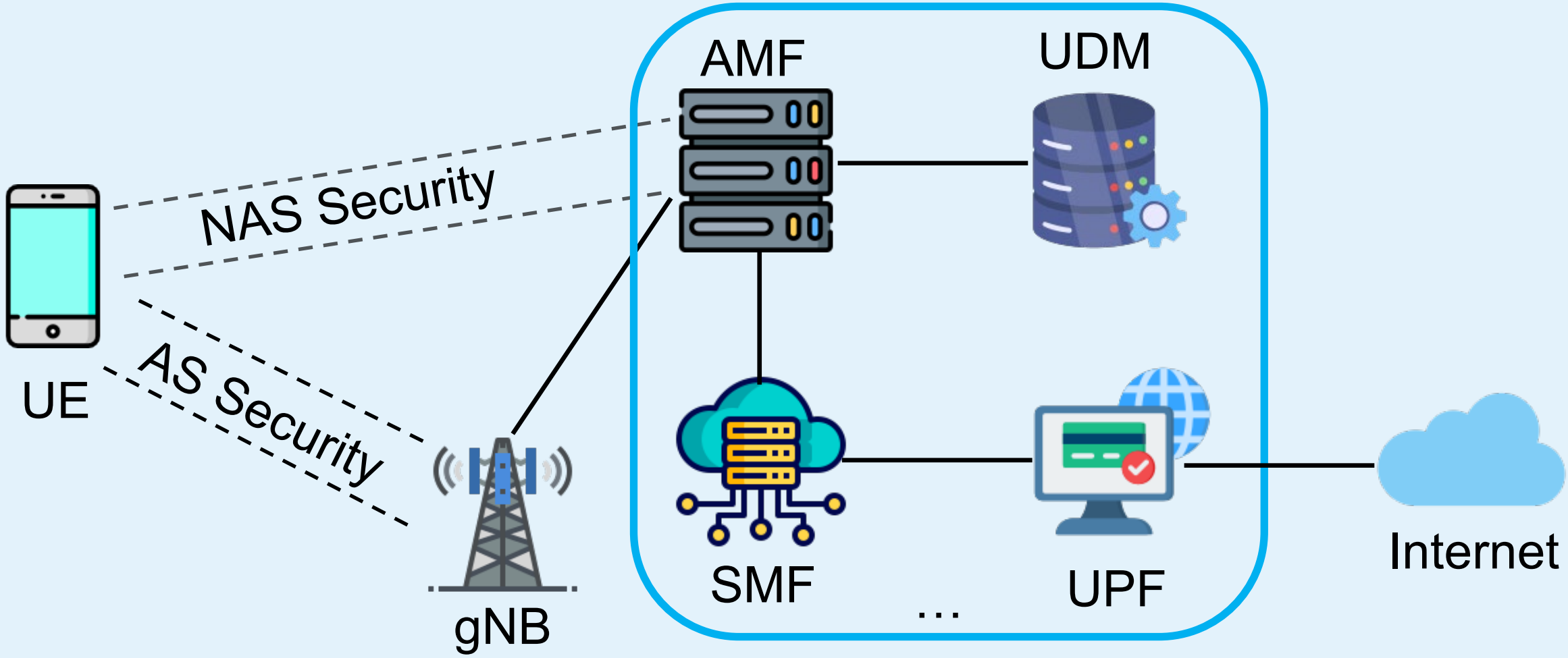
5G Network Architecture



5G Control Plane



Our Scope



#RSAC
RSAC 2025 Conference

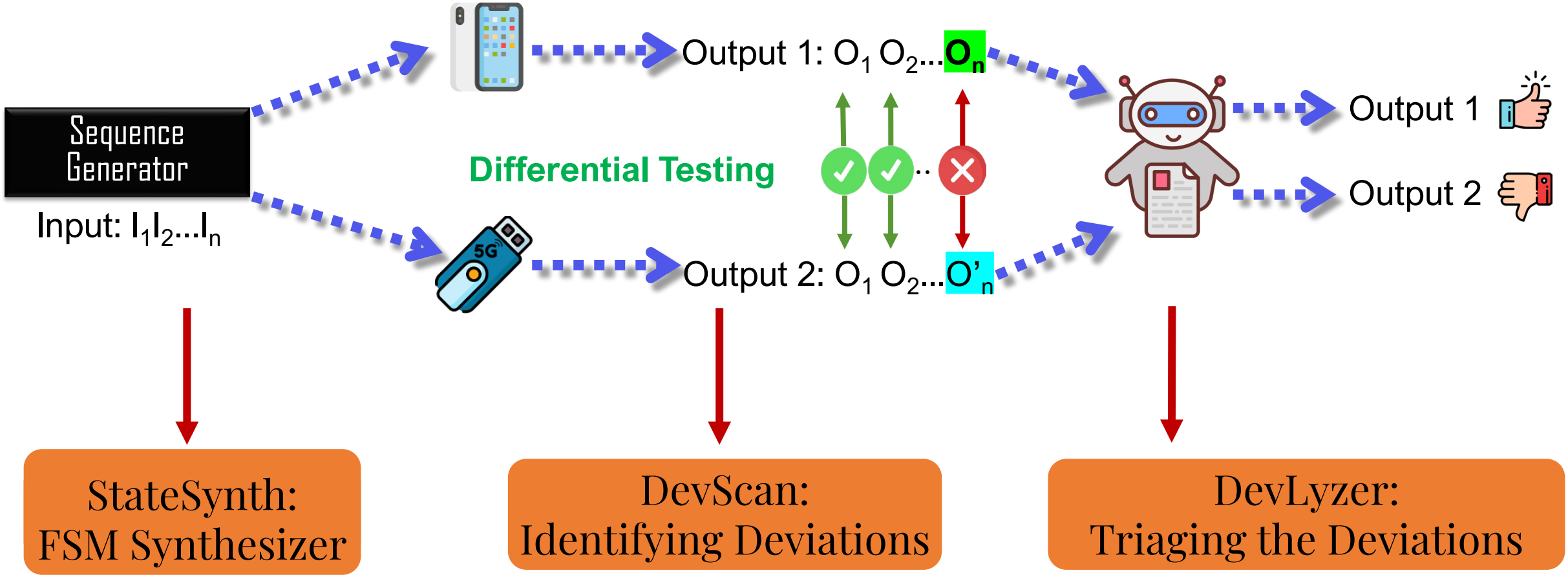
Our Goal

Is it possible to develop an automated framework to efficiently identify security policy violations in 5G UE control plane implementations?

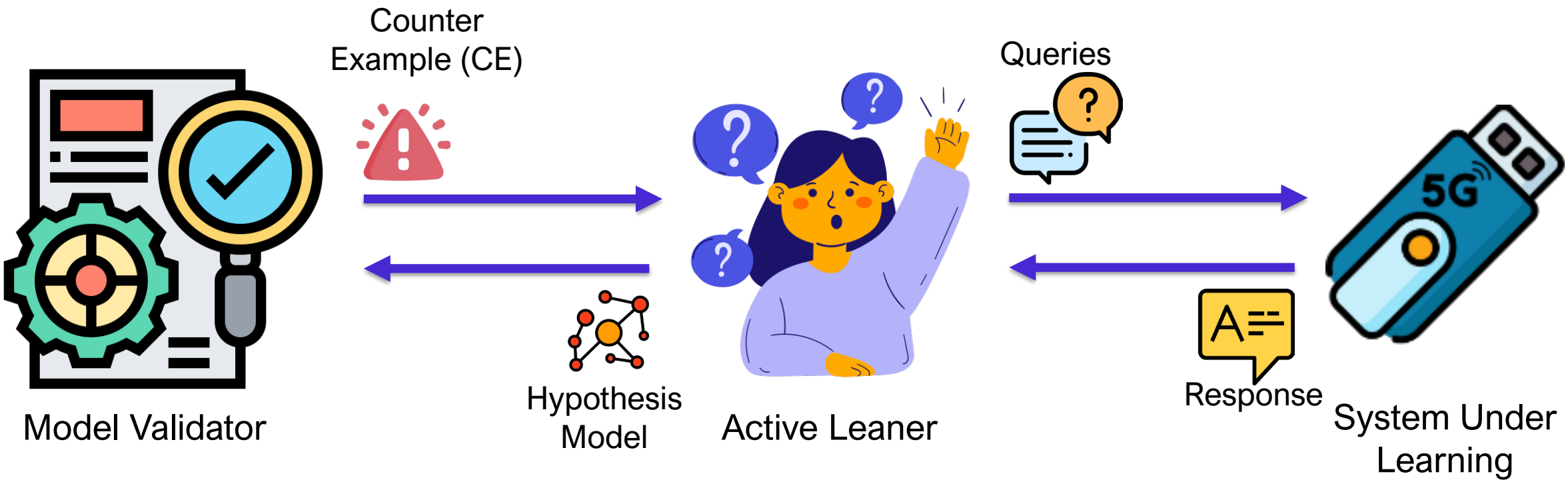
First Challenge

3GPP does not provide such a list which contains a complete set of security policies

High-level Philosophy of Our Approach



Active Automata Learning



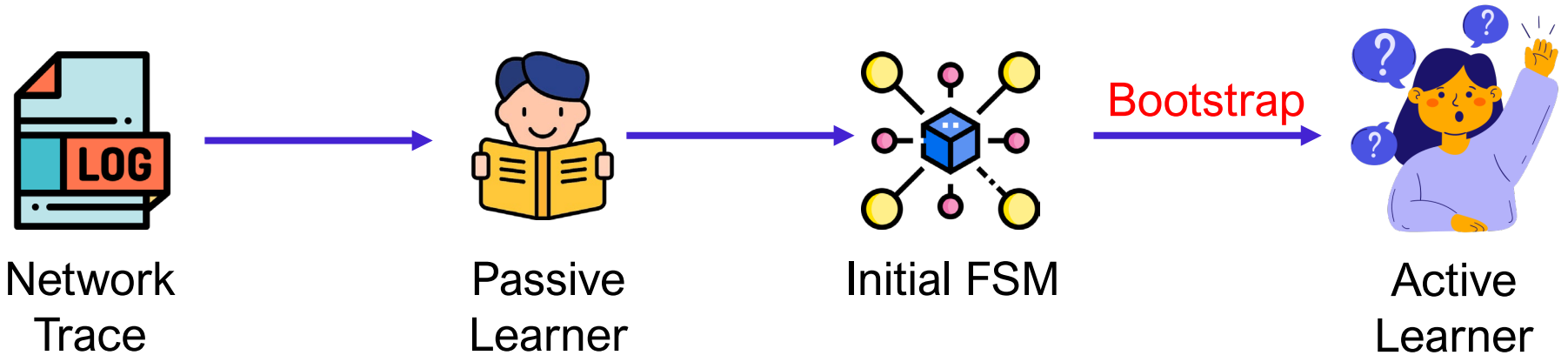
Challenges of Active Automata Learning

Active learner, initially does not have any idea about the 5G protocol interactions. It will generate many meaningless queries.

Large number of equivalence checking queries are generated in the model validation stage and most of them are not CE.

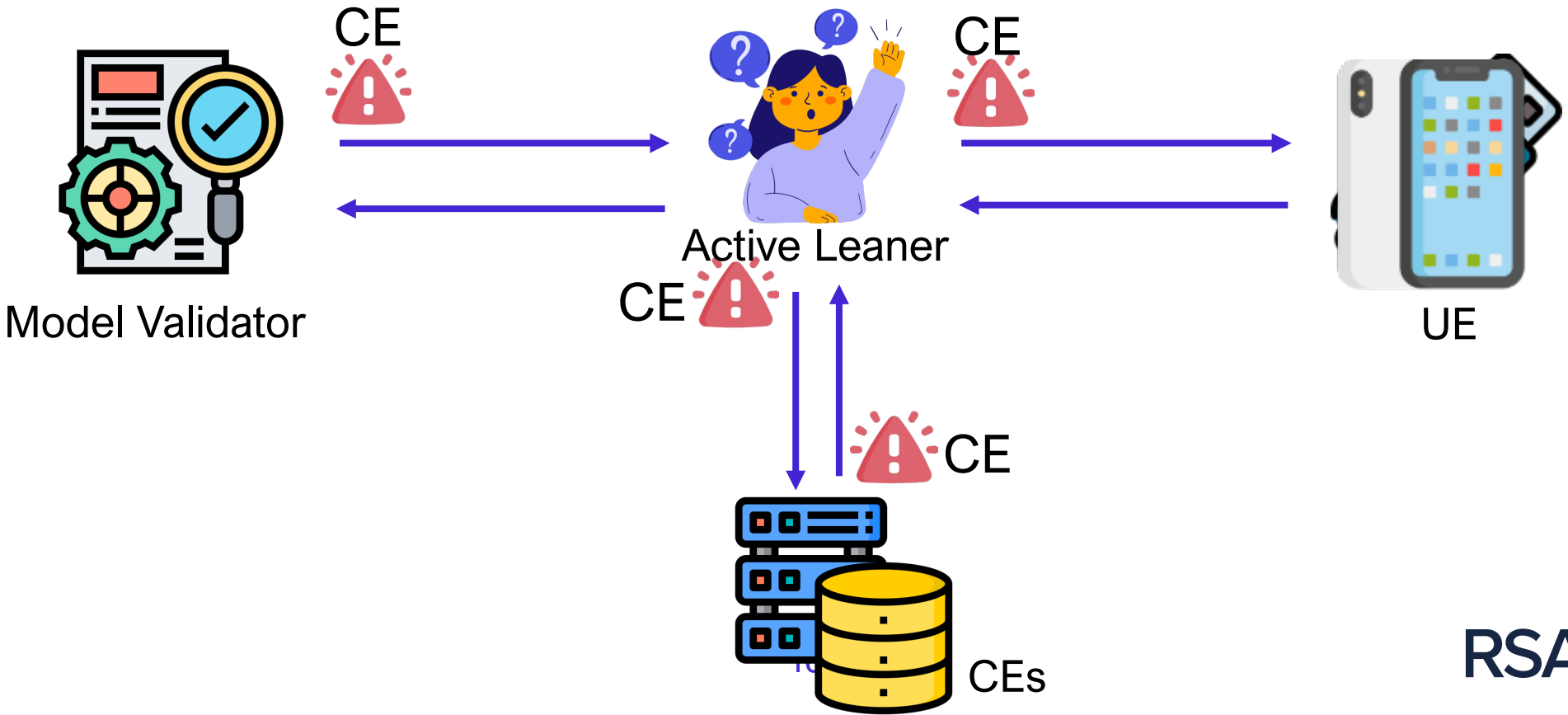
Hybrid Automata Learning

- Synthesize an initial FSM to provide guidance at the beginning of the active learning!

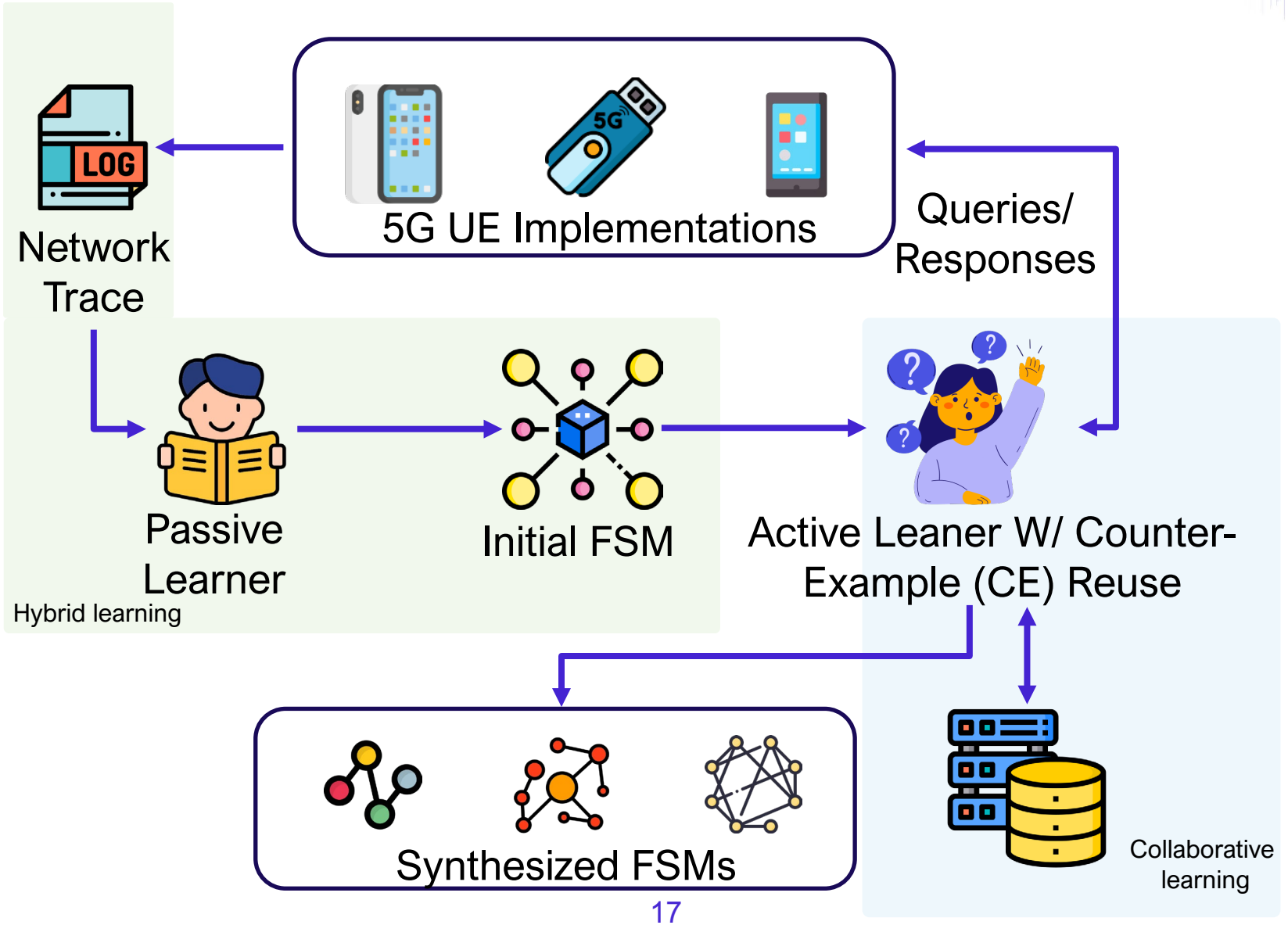


Collaborative Automata Learning

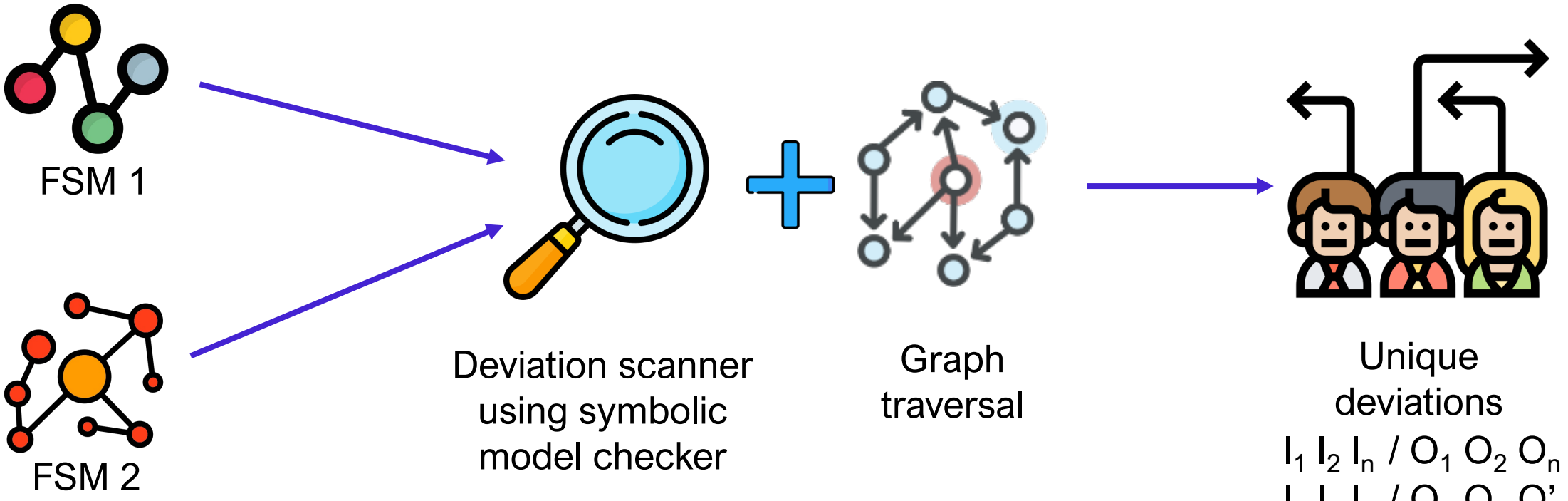
- Since all basebands implement the same protocol, and CEs found during FSM construction of one device are likely to be applicable to other basebands as well.



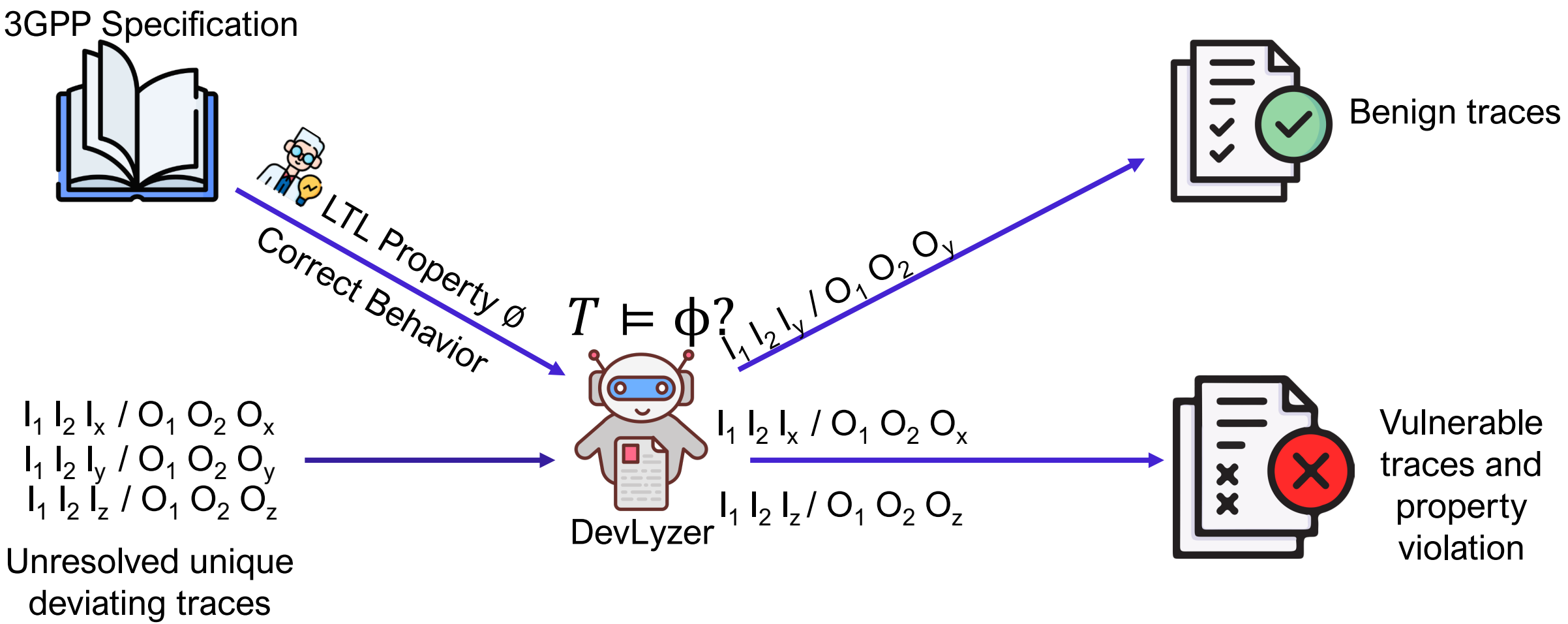
StateSynth: Workflow



DevScan: Workflow


FSM 1
FSM 2
Deviation scanner using symbolic model checker
Graph traversal
Unique deviations
$I_1\ I_2\ I_n\ /\ O_1\ O_2\ O_n$
$I_1\ I_2\ I_n\ /\ O_1\ O_2\ O'_n$

DevLyzer: Workflow


3GPP Specification
LTL Property ϕ
Correct Behavior
$T \models \phi$?
$I_1 I_2 I_y / O_1 O_2 O_y$
Benign traces
$I_1 I_2 I_x / O_1 O_2 O_x$
$I_1 I_2 I_y / O_1 O_2 O_y$
$I_1 I_2 I_z / O_1 O_2 O_z$
Unresolved unique deviating traces
DevLyzer
$I_1 I_2 I_x / O_1 O_2 O_x$
$I_1 I_2 I_z / O_1 O_2 O_z$
Vulnerable traces and property violation

LTL: Linear temporal logic

Evaluation

- We tested 17 Commercial Devices from 5 vendors + 2 Open-Source UE Implementations with 5GBaseChecker.

Qualcomm

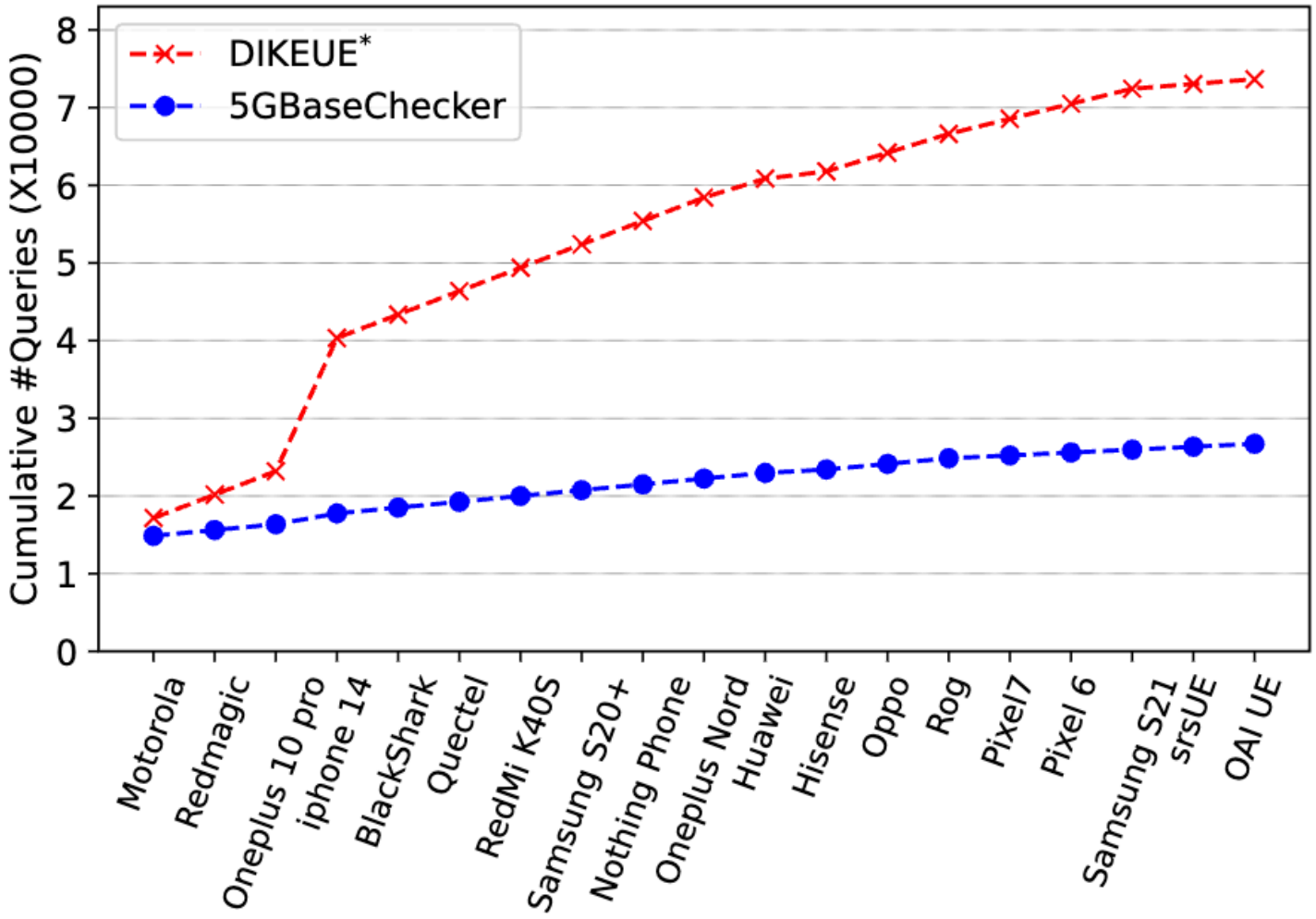
MEDIATEK

SAMSUNG Exynos

HISILICON

UNISOC®

Evaluation of StateSynth

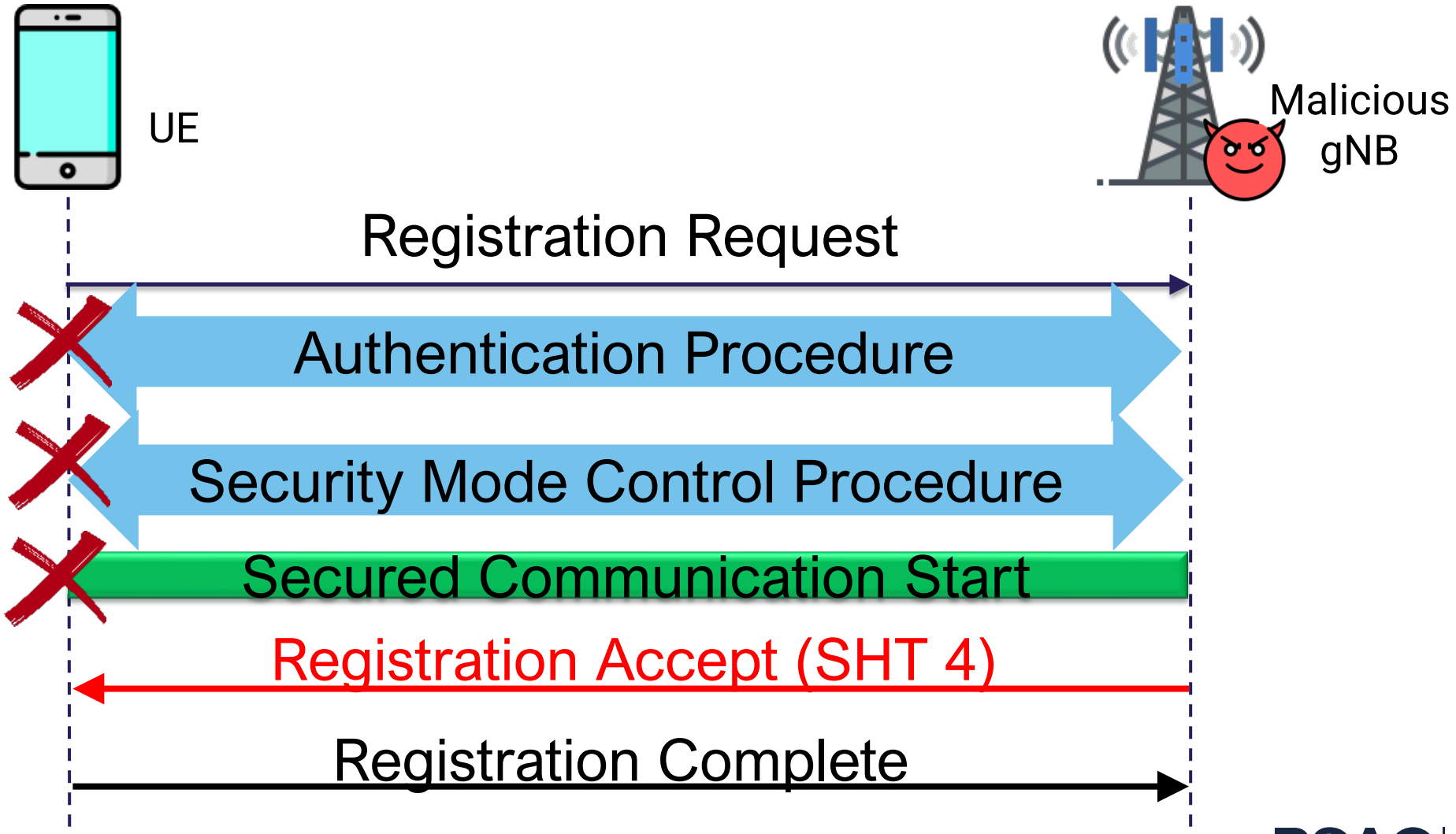


Findings and Impact

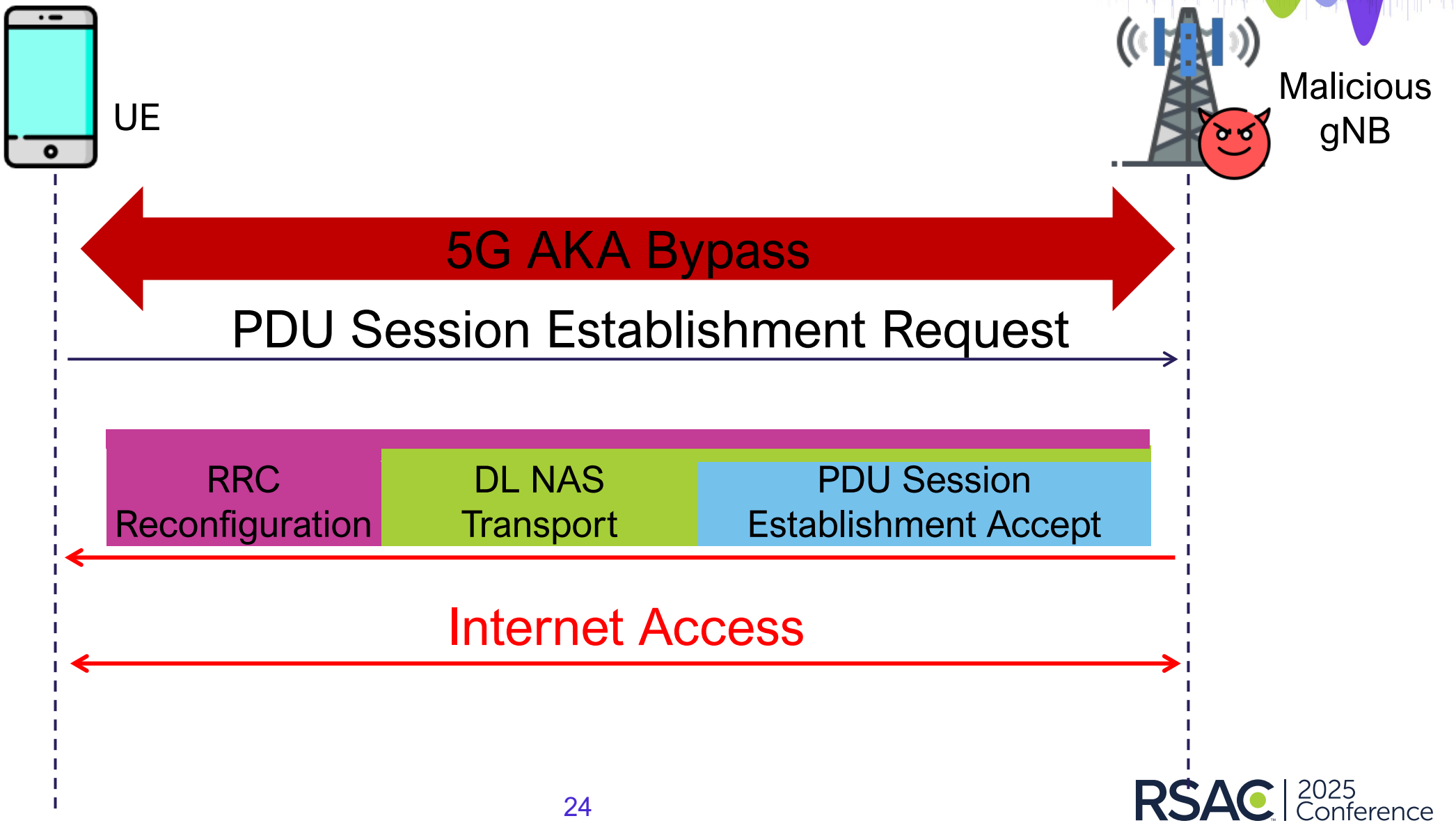
- Uncovered 22 unique issues, 13 could lead to exploitable attacks.
- 12 CVEs assigned and some vendor acknowledgements.
  - CVE-2023-52341, -49928, -50804, -49927, -50803, -52343, -52533, -52534, -52342, -52344; CVE-2024-29152, -28818
- GSMA Mobile Security Research Acknowledgements (CVD-2023-0081)

CVD-2023	0081	Kai Tu, Abdullah Al Ishtiaq, Syed MD Mukit Rashid, Yilu Dong, Weixuan Wang, Tianwei Wu, Syed Rafiul Hussain	Pennsylvania State University

5G AKA Bypass



Internet Traffic Eavesdropping



kai@kai: ~/Desktop/5GBaseChecker_Core

```
NN[internet] IPv4[10.45.0.2] IPv6[] (../src/sm
497)
04/06 20:19:47.410: [upf] INFO: [Added] Number of UPF-Sessions
is now 1 (../src/upf/context.c:178)
04/06 20:19:47.410: [gtp] INFO: gtp_connect()
(../lib/gtp/path.c:60)
04/06 20:19:47.410: [upf] INFO: UE F-SEID[CP:0x1 UP:0x1] APN[in
ternet] PDN-Type[1] IPv4[10.45.0.2] IPv6[] (../src/upf/context.
c:397)
04/06 20:19:47.410: [upf] INFO: UE F-SEID[CP:0x1 UP:0x1] APN[in
ternet] PDN-Type[1] IPv4[10.45.0.2] IPv6[] (../src/upf/context.
c:397)
04/06 20:19:47.410: [gtp] INFO: gtp_connect() [127.0.0.7]:2152
(../lib/gtp/path.c:60)
04/06 20:19:47.411: [amf] WARNING: 0x7f40a981c010 (../src/amf/n
amf-handler.c:83)
04/06 20:19:47.411: [sctp] INFO: sctp_senddata (../lib/sctp/ogs
-sctp.c:73)
04/06 20:19:47.446: [amf] INFO: number of events in queue 1 (..
/src/amf/event.c:106)
04/06 20:19:47.446: [gtp] INFO: gtp_connect() [127.0.0.5]:2152
(../lib/gtp/path.c:60)
04/06 20:19:47.446: [amf] INFO: set e->h.sbi.message (../src/am
f/amf-sm.c:511)
```

Attacker Terminal

kai@kai: ~/Desktop/clean/openairinter...

```
 CellGroup
[NR_MAC]   Activating RRC processing timer fo
ms
[NR_MAC]   (949.2) De-activating RRC processi
16
[NR_MAC]   Modified rnti 4a16 with CellGroup
[NR_MAC]   Added new CBRA process for UE RNTI 4a16 with initial
 CellGroup
[NR_RRC]   Receive RRC Reconfiguration Complete message UE 4a16
[PDCP]   ../../../openair2/LAYER2/nr_pdcp/nr_pdcp_oai_api.c:860
:add_drb_am: warning DRB 1 already exist for UE ID/RNTI 18966,
do nothing
[PDCP]   ../../../openair2/LAYER2/nr_pdcp/nr_pdcp_oai_api.c:add
_drb:911: added DRB for UE ID/RNTI 18966
[RLC]   ../../../openair2/LAYER2/nr_rlc/nr_rlc_oai_api.c:761:ad
d_drb_am: DRB 1 already exists for UE with RNTI 4a16, do nothin
g
[RLC]   ../../../openair2/LAYER2/nr_rlc/nr_rlc_oai_api.c:nr_rlc
_add_drb:860: added DRB to UE with RNTI 0x4a16
[NR_RRC]   [gNB 0] Frame  0 : Logical Channel UL-DCCH, Received
 NR_RRCReconfigurationComplete from UE rnti 4a16, reconfiguring
 DRB 1
[NR_RRC]   msg index 0, pdu_sessions index 0, status 2, xid 0):
 nb_of_pdusessions 1,  pdusession_id 5, teid: 1166204179
 [NR_RRC]   NGAP_PDUSESSION_SETUP_RESP: sending the message
[NGAP]   pdusession_setup_resp_p: pdusession ID 5, gnb_addr 127
.0.0.5, SIZE 4
[PDCP]   discard NR PDU rcvd_count=6, entity->rx_deliv 10,sdu_i
n_list 0
```

Attacker Terminal

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Trace Capture

ip.addr == 127.0.0.5 && dns || ngap || gtp

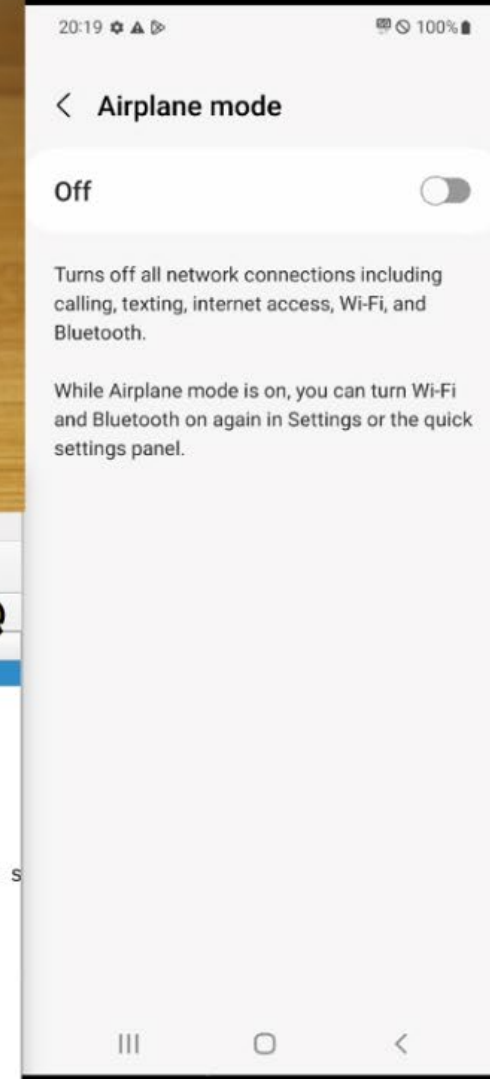
No.	Protocol	Info
961	NGAP	NGSetupRequest
963	NGAP	NGSetupResponse
3169	NGAP/N…	InitialUEMessage, Registration request, Registration request
3249	NGAP/N…	DownlinkNASTransport, Identity request
3255	NGAP/N…	SACK (Ack=1, Arwnd=106496) , UplinkNASTransport, Identity response
3340	NGAP/N…	DownlinkNASTransport, Registration accept
3351	NGAP/N…	SACK (Ack=2, Arwnd=106496) , UplinkNASTransport, Registration complete
3465	NGAP/N…	UplinkNASTransport, UL NAS transport, PDU session establishment request
3602	NGAP/N…	SACK (Ack=3, Arwnd=106496) , PDUSessionResourceSetupRequest, DL NAS transport, PDU s
3608	NGAP	SACK (Ack=4, Arwnd=106496) , PDUSessionResourceSetupResponse

Attack Message

Frame (118 bytes) Bitstring cvb (4 bytes) Unaligned OCTET STRING

Authentication Bypassed!!!

SM-G991B


20:19
100%
Airplane mode
Off
Turns off all network connections including calling, texting, internet access, Wi-Fi, and Bluetooth.
While Airplane mode is on, you can turn Wi-Fi and Bluetooth on again in Settings or the quick settings panel.

kai@kai: ~/Desktop/5GBaseChecker_Core

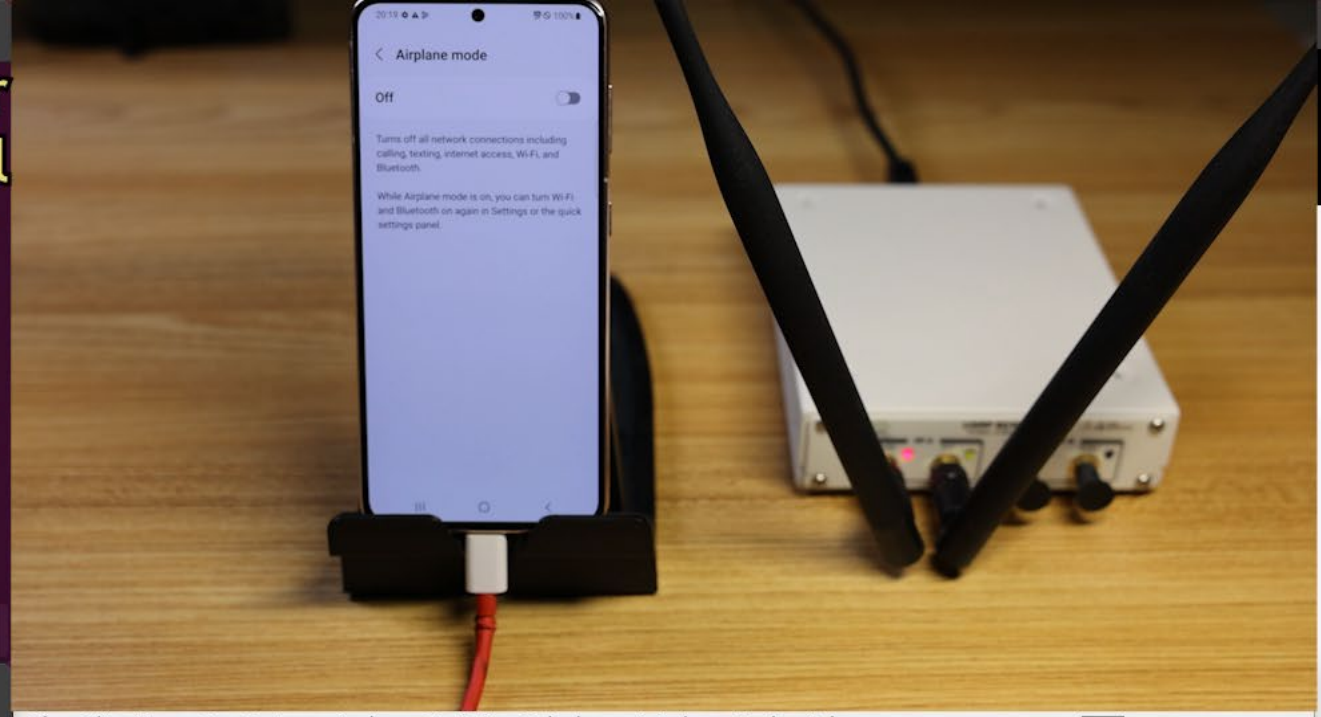
```
NN[internet] IPv4[10.45.0.2] IPv6[] (../src/smf/upf-handler.c:
497)
04/06 20:19:47.410: [upf] INFO: [Added] Number of UPF-Sessions
is now 1 (../src/upf/context.c:178)
04/06 20:19:47.410: [gtp] INFO: gtp_connect() [127.0.0.7]:2152
(../lib/gtp/path.c:60)
04/06 20:19:47.410: [upf] INFO: UE F-SEID[CP:0x1 UP:0x1] APN[in
ternet] PDN-Type[1] IPv4[10.45.0.2] IPv6[] (../src/upf/context.
c:397)
04/06 20:19:47.410: [upf] INFO: UE F-SEID[CP:0x1 UP:0x1] APN[in
ternet] PDN-Type[1] IPv4[10.45.0.2] IPv6[] (../src/upf/context.
c:397)
04/06 20:19:47.410: [gtp] INFO: gtp_connect() [127.0.0.7]:2152
(../lib/gtp/path.c:60)
04/06 20:19:47.411: [amf] WARNING: 0x7f40a981c010 (../src/amf/n
amf-handler.c:83)
04/06 20:19:47.411: [sctp] INFO: sctp_senddata (../lib/sctp/ogs
-sctp.c:73)
04/06 20:19:47.446: [amf] INFO: number of events in queue 1 (..
/src/amf/event.c:106)
04/06 20:19:47.446: [gtp] INFO: gtp_connect() [127.0.0.5]:2152
(../lib/gtp/path.c:60)
04/06 20:19:47.446: [amf] INFO: set e->h.sbi.message (../src/am
f/amf-sm.c:511)
```

Attacker Terminal

kai@kai: ~/Desktop/clean/openairinter...

```
harq rounds)
[NR_MAC]   handle harq for rnti 636f, in RA p
[NR_MAC]   handle_nr_ul_harq(): unknown RNTI 0x636f in PUSCH
[NR_PHY]   [gNB 0][RAPROC] Frame 79, slot 19
edure with preamble 5, energy 51.0 dB (I0 136,
y 9 start symbol 0 freq index 0
[NR_PHY]   [gNB 0][RAPROC] Frame 79, slot 19 Initiating RA proc
edure with preamble 41, energy 51.0 dB (I0 180, thres 120), del
ay 10 start symbol 4 freq index 0
[NR_PHY]   [gNB 0][RAPROC] Frame 79, slot 19 Initiating RA proc
edure with preamble 0, energy 48.0 dB (I0 219, thres 120), dela
y 20 start symbol 8 freq index 0
[MAC]   UL_info[Frame 79, Slot 19] Calling initiate_ra_proc RAC
H:SFN/SLOT:79/19
[NR_MAC]   [gNB 0][RAPROC] CC_id 0 Frame 79 Activating Msg2 gen
eration in frame 80, slot 7 using RA rnti 10b SSB, new rnti d8d
4 index 0 RA index 0
[NR_MAC]   [gNB 0][RAPROC] FAILURE: CC_id 0 Frame 79 initiating
 RA procedure for preamble index 0
[MAC]   UL_info[Frame 80, Slot 0] Calling initiate_ra_proc RACH
:SFN/SLOT:79/19
[NR_MAC]   [gNB 0][RAPROC] FAILURE: CC_id 0 Frame 79 initiating
 RA procedure for preamble index 0
[NR_MAC]   [gNB 0][RAPROC] CC_id 0 Frame 80, slotP 7: Generatin
g RA-Msg2 DCI, rnti 0x10b, state 1, CoreSetType 2
[NR_MAC]   [RAPROC] Msg3 slot 17: current slot 7 Msg3 frame 80
k2 7 Msg3_tda_id 3
[NR_MAC]   [gNB 0][RAPROC] Frame 80, Subframe 7: rnti d8d4 RA s
tate 2
```

Attacker Terminal



File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Trace Capture

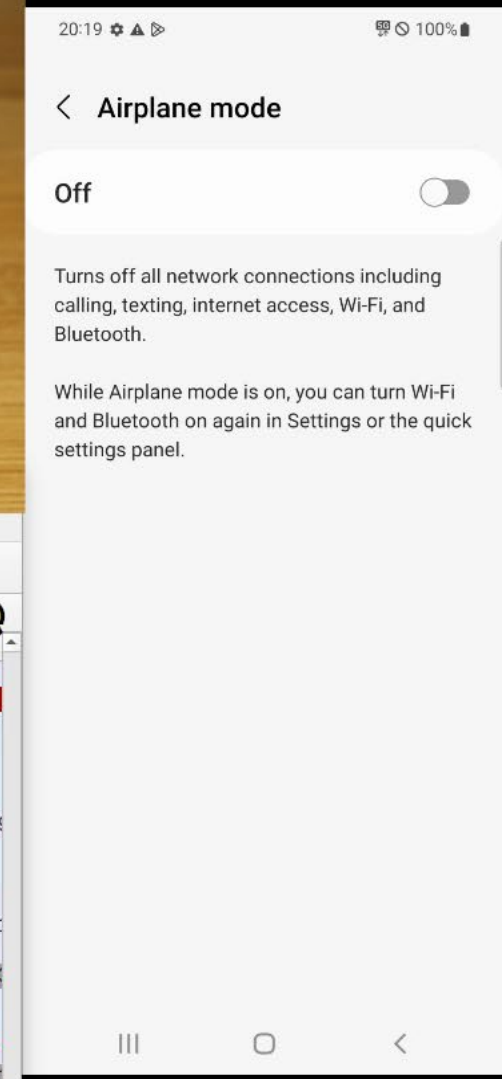
ip.addr == 127.0.0.5 && dns || ngap || gtp

No.	Protocol	Info
3856	GTP <T…	Application Data
3857	GTP <T…	443 → 37814 [RST] Seq=1009 Win=0 Len=0
3868	GTP <D…	Standard query response 0x8467 AAAA b4E8Sm-dnsotls-ds.metric.gstatic.com AAAA 2607
3869	GTP <Q…	Protected Payload (KP0), DCID=ee7412ff33df9008
3870	GTP <Q…	Protected Payload (KP0), DCID=ee7412ff33df9008
3871	GTP <Q…	Protected Payload (KP0), DCID=ee7412ff33df9008
3872	GTP <T…	45302 → 853 [ACK] Seq=373 Ack=5429 Win=78848 Len=0 TSval=2231640716 TSecr=3869412
3885	GTP <Q…	Protected Payl (KP0), DCID=5acfc1d1af97e6fb1c73a7d7c92efc6d7f9d4e8e
3886	GTP <D…	Standard query dbc7 AAAA K5j3NM-dnsotls-ds.metric.gstatic.com
3887	GTP <T…	Application Da
3888	GTP <T…	33348 → 853 [eq=451 Ack=5535 Win=79872 Len=0 TSval=1335136228 TSecr=7613728
3889	GTP <T…	Application Dat
3890	GTP <T…	33348 → 853 [FIN, ACK] Seq=475 Ack=5535 Win=79872 Len=0 TSval=1335136234 TSecr=761
3891	GTP <D…	Standard query 0xa357 A youtubei.googleapis.com
3902	GTP <D…	Standard query response 0xdbc7 AAAA K5j3NM-dnsotls-ds.metric.gstatic.com AAAA 260
3903	GTP <T…	Application Data
3904	GTP <T…	853 → 33348 [FIN, ACK] Seq=5535 Ack=475 Win=67840 Len=0 TSval=761373029 TSecr=1335
3905	GTP <T…	853 → 33348 [ACK] Seq=5536 Ack=476 Win=67840 Len=0 TSval=761373031 TSecr=133513623
3906	GTP <D…	Standard query response 0xa357 A youtubei.googleapis.com A 142.251.40.138 A 142.25
3907	GTP <Q…	Initial, DCID=aa5c42630c886a78, PKN: 1, CRYPTO, CRYPTO, PADDING, PING, CRYPTO, PADD

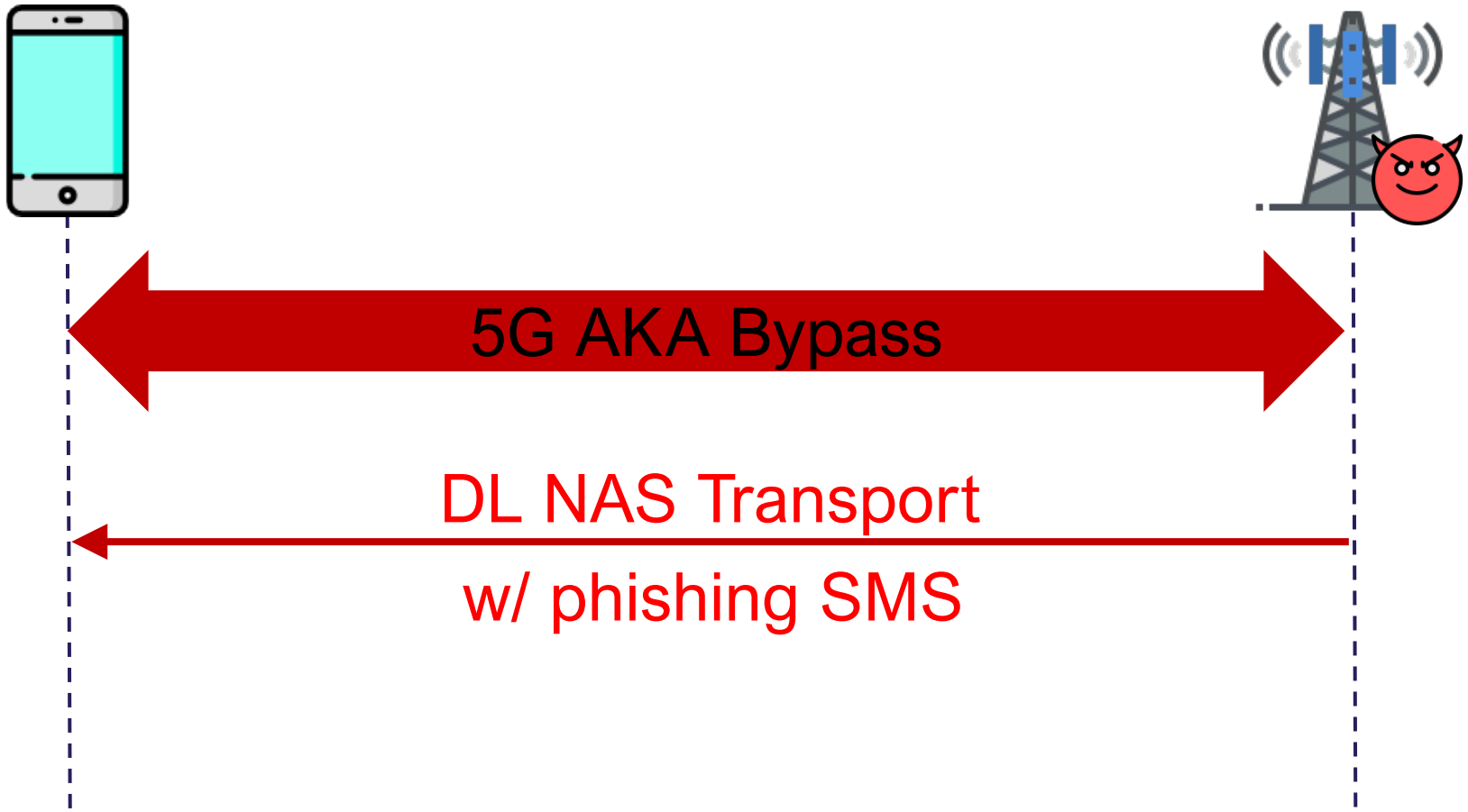
Plaintext DNS Packets

Frame (118 bytes) Bitstring CVD (4 bytes) Unaligned OCTET STRING

SM-G991B


20:19
100%
Airplane mode
Off
Turns off all network connections including calling, texting, internet access, Wi-Fi, and Bluetooth.
While Airplane mode is on, you can turn Wi-Fi and Bluetooth on again in Settings or the quick settings panel.

Phishing SMS Injection



kai@kai: ~/Desktop/5GBaseChecker_Core

```
04/06 19:57:01.609: [sbi] INFO: [5c89a00a-f471-
c0f059] NF registered [Heartbeat:1s] (../lib/
04/06 19:57:03.706: [smf] WARNING: PFCP[REQ] has already been a
ssociated (../src/smf/pfcp-sm.c:213)
04/06 19:57:03.707: [upf] WARNING: PFCP[RSP] h
ssociated (../src/upf/pfcp-sm.c:207)
04/06 19:57:04.273: [amf] INFO: gNB-N2 accepted[127.0.0.1]:4775
2 in ng-path module (../src/amf/ngap-sctp.c:113)
04/06 19:57:04.273: [amf] INFO: number of events in queue 1 (..
/src/amf/event.c:106)
04/06 19:57:04.273: [amf] INFO: gNB-N2 accepted[127.0.0.1] in m
aster_sm module (../src/amf/amf-sm.c:720)
04/06 19:57:04.273: [amf] INFO: [Added] Number of gNBs is now 1
 (../src/amf/context.c:881)
04/06 19:57:04.273: [amf] INFO: number of events in queue 1 (..
/src/amf/event.c:106)
04/06 19:57:04.273: [amf] INFO: gNB-N2[127.0.0.1] max_num_of_os
treams : 2 (../src/amf/amf-sm.c:759)
04/06 19:57:04.273: [amf] INFO: number of events in queue 1 (..
/src/amf/event.c:106)
04/06 19:57:04.273: [sctp] INFO: sctp_senddata (../lib/sctp/ogs
-sctp.c:73)
04/06 19:57:13.281: [amf] INFO: buffer:Hello
 (../src/amf/testsocket.c:248)
```

Attacker Terminal

kai@kai: ~/Desktop/clean/openairinter...

```
got sync (ru_thread)
got sync (L1_stats_thread)
[HW]   current pps at 2.000000, starting streaming at 3.000000
[PHY]   RU 0 rf device ready
[PHY]   RU 0 RF started opp_enabled 0
initializing tx write thread
end of tx write thread
[UTIL]   Creating thread trx_usrp_write_thread with affinity -1
 and priority 97
[PHY]   tx write thread ready
trx_usrp_write_thread started on cpu 1
sleep...
sleep...
sleep...
sleep...
sleep...
sleep...
sleep...
sleep...
sleep...
sleep...
[PHY]   tx_reorder_thread started
[NR_MAC]   Frame.Slot 384.0

[NR_MAC]   Frame.Slot 512.0

[NR_MAC]   Frame.Slot 640.0

[NR_MAC]   Frame.Slot 768.0
```

Attacker Terminal

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

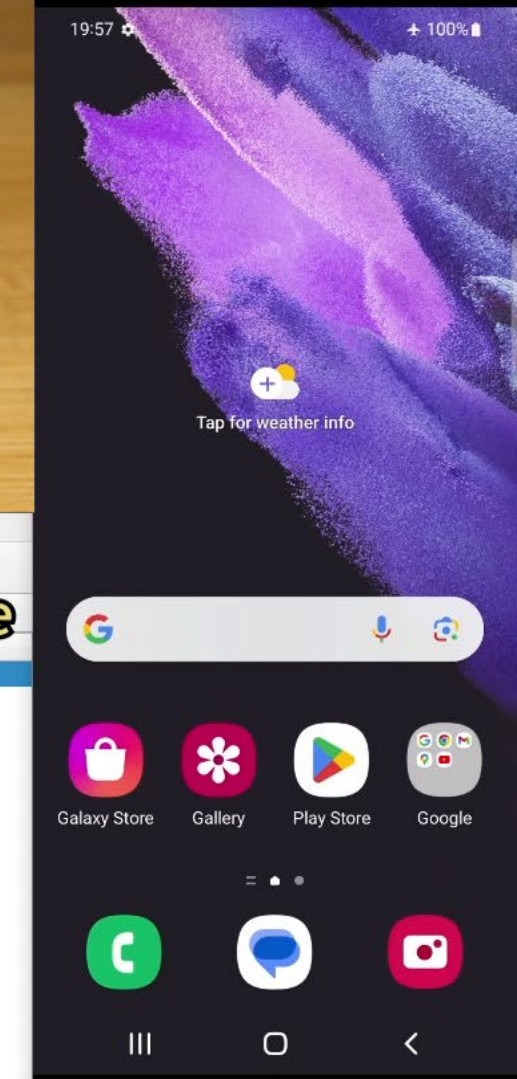
ip.addr == 127.0.0.5 && dns || ngap || gtp

No.	Protocol	Info
4473	NGAP	NGSetupRequest
4475	NGAP	NGSetupResponse

Frame (118 bytes) Bitstring cvb (4 bytes) Unaligned OCTET STRING

Trace Capture

SM-G991B



Takeaways

- More security-focused tests are required before shipping the modem products.
- Black-box testing is an efficient method for detecting logical bugs as it requires only input and output analysis, making it more scalable and convenient compared to emulation or rehosting-based approaches.
- We open-sourced our tool 5GBaseChecker at: github.com/SyNSec-den/5GBaseChecker

RSAC 2025 Conference

Many Voices.
One Community.

Thanks! Q&A?

Kai Tu

Email: kjt5562@psu.edu

Website: hellotkk.github.io